CLAIMS

1. A security intrusion mitigation method comprising:

utilizing network spanning tree configuration information to determine an action for mitigating diffusion of intrusive attacks, wherein said spanning tree information includes an indication of an internal diffusion risks; and

performing said action for mitigating diffusion of intrusive attacks automatically, wherein said action for mitigating includes compensation for functional support of prioritized applications.

2. A security intrusion mitigation method of Claim 1 further comprising utilizing said internal diffusion risk values to determine components forming a path in said spanning tree configuration with a highest cumulative diffusion impact risk.

3. A security intrusion mitigation method of Claim 1 wherein said internal diffusion risk includes an asset value factor.

4. A security intrusion mitigation method of Claim 3 wherein said asset value corresponds to an economic impact of a disruption to functionality provided by a network component.

5. A security intrusion mitigation method of Claim 1 wherein said internal diffusion risk includes an exposure rating factor.

6. A security intrusion mitigation method of Claim 5 wherein said exposure rating defines a threshold value corresponding to connectivity of a network component with other network components.

7. A security intrusion mitigation method of Claim 5 wherein said network component is assigned an exposure rating value based upon a connectivity distance from a root node.

8. A security intrusion mitigation method of Claim 5 wherein said action for mitigating diffusion of intrusive attacks is implemented in accordance with a highest risk algorithm.

9. A security intrusion mitigation method of Claim 5 wherein said network spanning tree configuration information includes information associated with components included in a utility data center and said mitigation action is implemented in said utility data center.

10. A security intrusion mitigation system comprising:

a means for communicating information;

a means for processing said information including instructions for determining a highest risk path and automatically mitigating an attack spread to components included in said highest risk path; and

a means for storing said information, including instructions determining a highest risk path and automatically mitigating an attack spread to components included in said highest risk path.

11. A security intrusion mitigation system of claim 10 wherein said instructions include security management instructions implemented on a network application management platform.

12. A security intrusion mitigation system of claim 10 further comprising a means for interfacing with a network application management platform.

13. A security intrusion mitigation system of claim 10 wherein said instructions include attack spread risk determination instructions.

14. A security intrusion mitigation system of claim 10 further comprising a means for centrally controlling a utility data center operations.

15. A computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement security intrusion mitigation instructions comprising:

a component risk determination module for determining a risk of an attack spreading from a first component to a second component included in a network; and

an attack spreading response module for responding to said risk of an attack spreading from a first component to a second component included in said network.

16. A computer usable storage medium of Claim 15 wherein said risk is biased based upon an economic value of functions said second component performs.

17. A computer usable storage medium of Claim 15 said risk is biased based upon connectivity of said second component to said first component in said network.

18. A computer usable storage medium of Claim 17 wherein said response includes reducing traffic communication to said second component.

19. A computer usable storage medium of Claim 15 wherein said response includes turning off an interface of said second component to said network.

20. A computer readable medium of Claim 19 wherein said response is performed in accordance with an highest risk analysis.